Science and Technology Law Review

Volume 17 | Number 2 Article 6

2014

Revenge: Free of Charge

Salina Tariq

Revenge: Free of "Charge?"

*Salina Tariq**

I. Introduction

The Internet era began in the 90s and brought with it an entirely unforeseeable arena for crime and business. One consequence was the commercialization of personal offenses. The hosting of illegal communication has recently become a business enterprise. The website MyEx.com is a prime example.[1] Who can argue that with a name like that, the service provider is bound to know that the postings will be non-consensual and used to harass people and cause them emotional distress? Once material is posted, a victim may have the images removed by logging onto a sister website and paying a $500 removal fee.[2] There are various posts by individuals, often the posters of the material themselves, on Google Groups desperately trying to remove offensive material from the website, but they are unable to afford the high removal fees.[3] The material shows up in a simple Google search, yet Google has no duty to remove the images from its search engine even if it learns that the sexually explicit images are in fact distributed without the owner's consent.[4] Federal laws have recently incorporated cybercrimes within their context, but prosecuting harassers and bullies has not been successful. The lack of success may be a result of the difficulty in locating the defendant. For example, the MyEx.com website is hosted in the Netherlands, but registered in Hong Kong, and removal payments are sent to a company in the Philippines that repairs online reputations.[5] The widespread and global use of the Internet has brought with it vast quantities of comprehensive knowledge and means for communication at everyone's fingertips. However, this great benefit has not come without a price. The high cost of Internet usage is one that our law enforcement mechanisms have dramatically failed to keep up with and compensate for.

---

* Salina Tariq is an August 2014 Candidate for Juris Doctor at SMU Dedman School of Law. She received her Bachelor of Arts Degree in Criminology from the University of Texas at Arlington in 2007. Salina would like to thank her mother for her unconditional love and support, and the rest of her family for their continuous patience and encouragement.

1. *See* Danica Johnson, *Taking a Stand against Revenge Porn and Internet Exploitation in the Digital Age*, Everyday Feminism (Dec. 3, 2013), http://everydayfeminism.com/2013/12/revenge-porn-and-internet-exploitation.

2. *Id.*

3. *See* Removing Content, Google Groups, https://productforums.google.com/forum/#!topic/webmasters/Ida46SOYq1c%5B1-25-false%5D.

4. *See* Communications Decency Act of 1996, 47 U.S.C. § 230 (c) (2006).

5. Mark Markovich, *Revenge Porn Websites Taking Advantage of Weak Privacy Laws*, KomoNews.Com (Nov. 21, 2013), http://www.komonews.com/news/local/Privacy-Laws-Weak-at-Protecting-Nude-Photos-on-Revenge-Porn-Websites-232935541.html.

The U.S. Supreme Court, in the ground breaking case *Reno v. American Civil Liberties Union (ACLU)*, held that interfering with the rights of adults to communicate and receive indecent and patently offensive material over the Internet was a violation of the First Amendment.[6] The Court, therefore, gave Internet pornography the same highest protection allowed under the First Amendment as that held by print media.[7] Following the same warped understanding of pornography as an accepted form of speech and expression and the First Amendment right to publish such forms of artistic expression, courts and legislation seem to have given full immunity to web service providers from claims of non-consensual displays of private content and information. Perhaps the legal system was worried that First Amendment protection was not sufficient in protecting the expression of pornography that every American deserves to enjoy without having to search too hard. It deemed it a creative endeavor and gave it additional protection, and economic incentive, under the Copyright Act.

It is too harsh to say that the legal system has been unwilling to provide any solace to the victims of unauthorized disclosures of pornographic materials; legal action is possible under criminal and tort law. Federal and state cyber harassment criminal laws and tort remedies have been utilized to punish the distributors of revenge porn. But, not much success has been gained due to the somewhat confidential nature of Internet postings and the First Amendment protections enjoyed by service providers who have no duty to disclose the distributor's identity. Where successful actions have been brought against the vengeful initial culprits responsible for making the material go viral, the victim cannot be reasonably compensated for injuries suffered. First, once the materials find their way to the website, it is impossible to retract the material and make it disappear. Second, the initial culprits are usually ex-lovers who do not have any meaningful assets that could compensate the victim monetarily. After all, the actual beneficiaries of the destructive pornographic material have been granted such protection that there are no means for recovery.

This is not to say that law enforcement agents have not had any success in bringing down website providers. In January 2014, FBI agents arrested Hunter Moore, a revenge porn tycoonand founder of the website "Is Anyone Up."[8] The website is known for posting nude pictures without the subject's consent.[9] The website has been accused of extortion several times.[10] The indictment also names Moore's accomplice, Charles Evans for conspiracy to

6. Reno v. ACLU, 521 U.S. 844 (1997).

7. *See generally id.*

8. Russell Brandom, *Revenge Porn Magnate Hunter Moore has been Arrested by the FBI*, THE VERGE (Jan. 23, 2014), http://www.theverge.com/2014/1/23/5338694/revenge-porn-magnate-hunter-moore-has-been-arrested-by-the-fbi.

9. *Id.*

10. *Id.*

"access a protected computer without authorization to obtain information for private gain."[11] This alleged action falls within the Computer Fraud and Abuse Act.[12] The charge followed after Evans hacked into a user's email account to obtain nude photographs which were then sold to Moore and posted on the website.[13] The cause of action against Moore arose when he offered to pay $250 for the images.[14]

This article will focus on the road that has led to the virtual indestructibility of the Internet pornographer and those who create a venue for its display. Part II will provide a brief overview of the legal status of pornography, from obscene to constitutionally protected expression, and ultimately to a copyrightable entity; a useful form of art. Part III will illustrate the current state of the law as it pertains to non-consensual distribution of pornography and Internet service provider immunity. The section will point out the deficiencies in the legal system and the inadequacy of legal remedies available to victims. Finally, the section will compare United States law to some of the more victim-friendly laws of foreign countries. Part IV will outline a number of proposals that have the potential to deter the unauthorized distribution of pornography, thereby providing relief to current and future victims.

II. HISTORICAL BACKGROUND

A. Pornography's Journey from Obscenity to Protected Speech to Copyrightable Enterprise

Historically, the legal focus on Internet regulation has been largely aimed at protecting unauthorized use of copyrighted audio and video works.[15] The lack of initiative toward protecting victims of non-consensual distribution of pornography has been partly caused by society's failure to accept non-consensual pornography as a serious danger, having somewhat regarded it as a victimless crime. Blame is placed on individuals who willingly produced the sexual images and then passed along to their intimate partners.[16] But, regardless of whether society believes that the victims "had it coming," placing undeserved trust in one's spouse or lover is not an act wor-

11. *Id.*

12. *Id.*

13. *Id.*

14. Brandom, *supra* note 8.

15. Anne Bartow, *User-Generated Confusion: The Legal and Business Implications of Web 2.0: Vanderbilt Journal of Entertainment and Technology Law 10th Anniversary Symposium: Article: Pornography, Coercion and Copyright Law 2.0*, 10 VAND. J. ENT. & TECH. L. 799, 800 (2008).

16. Ariel Ronneburger, *Sex, Privacy, and Webpages: Creating a Legal Remedy for Victims of Porn 2.0*, SYRACUSE SCI. & TECH. L. REP. 1, 10 (2009).

thy of the suffering brought about by revenge porn.[17] After all, our legal system has continuously emphasized the valued principle of consent.[18]

Where First Amendment protection of freedom of speech and expression comes into play in the context of pornography, historically such sexually explicit material had been granted no constitutional protection under the argument that obscene works are not covered under First Amendment.[19] In 1957 the Supreme Court noted:

> All ideas having even the slightest redeeming social importance—unorthodox ideas, controversial ideas, even ideas hateful to the prevailing climate of public opinion—have full protection of the guaranties [of speech and press] . . . . But implicit in the history of the First Amendment is the rejection of obscenity as utterly without redeeming social importance.[20]

This notion of equating pornography to obscenity, unworthy of constitutional protection, was supported by the fact that most states at the time prosecuted offenses of libel, blasphemy, and profanity on the understanding that such related conduct was obscenity specifically excepted from First Amendment protection.[21] The regulation of pornography at that time mainly focused on the offensive and obscene nature of pornographic material and had not much to do with its propensity to cause actual harm.[22]

Gradually, however, the rationale behind curtailing the right to freedom of speech under a general obscenity analysis no longer satisfied critics of sexual censorship.[23] It therefore became important to regulate pornography under the contention that it caused harm to society, the kind of harm from which the government has a substantial interest in protecting citizens.[24]

In 1984, the Indianapolis City Council took the first important step toward creating pornography regulations focusing on the harmful effects of the material.[25] Andrea Dworkin and Catherine MacKinnon drafted the legislation that defined pornography as "the graphic sexually explicit subordination of women, whether in pictures or in words."[26] The ordinance saw some success

17. *Id.*

18. *Id.*

19. *See* Roth v. United States, 354 U.S. 476, 484 (1957).

20. *Id.*

21. Mark Huppin & Neil Malamuth, *Adult Entertainment: The Obscenity Conundrum, Contingent Harms, and Constitutional Consistency*, 23 STAN. L. & POL'Y REV. 31, 44–45 (2012).

22. *Id.* at 54.

23. *Id.*

24. *Id.*

25. *Id.*

26. *Id.* at 55.

at the local level, but it ultimately failed to become American law.[27] Following this failed attempt to provide subjects of pornography compensation for their harm, and based on similar arguments, came the Pornography Victims Compensation Act.[28] The Act provided victims of sexual assault the legal ability to sue distributors of obscene material and child pornography.[29] The Bill was introduced to the Senate in 1991 by Senator Mitch McConnell, and was approved by the Judiciary Committee in 1992 in a slightly modified form.[30] The Bill was widely criticized for shifting blame from actual murderers and rapists to pornography distributors.[31] In 1990, influenced by the Bill, Illinois passed a civil liability statute that allows victims of sex crimes to bring civil suits.[32] However, this legislation was simply geared towards providing civil remedies to victims of sexual crimes and did nothing to protect the subjects of non-consensual pornography.

In 1997, forty years after the Supreme Court found that pornographic material was not afforded First Amendment protection due to its obscene nature,[33] the Court in *Reno v. ACLU* took an entirely opposite stance and found that unduly burdening the rights of adults to communicate and receive indecent and offensive material over the Internet was a violation of the First Amendment.[34] In doing so, the Court gave Internet communications the highest form of First Amendment protection, which waspreviously enjoyed only by print media.[35] In this landmark case, the Supreme Court agreed with respondents that certain provisions of the CDA violated the First Amendment by restricting the rights of adults to provide and receive indecent material.[36] The Court argued that many sexually explicit communications, although indecent and offensive, were not obscene.[37] The Court, in defining obscenity

27. Huppin & Malamuth, *supra* note 21, at 55.

28. Marianne Wesson, *Girls Should Bring Lawsuits Everywhere . . . Nothing Will Be Corrupted: Pornography as Speech and Product*, 60 U. CHI. L. REV. 845, 850 (1993) (quoting S. 1521, 102d Cong, 1st Sess, in 137 Cong Rec 10554 (July 22, 1991)).

29. *Id.*

30. *Id.* (discussing S. 1521, 102d Cong, 2d Sess, in 138 Cong Rec 12570 (Aug 12, 1992)).

31. *Id.*

32. *Id.*

33. *See* Roth v. United States, 354 U.S. 476, 484 (1957).

34. Reno v. ACLU, 521 U.S. 844, 874 (1997).

35. Rebecca Jacubcin, comment, Reno v. ACLU*: Establishing a First Amendment Level of Protection for the Internet*, 9 U. FLA. J. L. & PUB. POL'Y 287, 287–88 (1998).

36. *Reno*, 521 U.S. at 874.

37. *Id.* at 873.

set forth a test in *Miller v. California* to determine whether something fell within that term.[38] This three-part test is:

> (a) whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.[39]

Distinguishing Internet communications from other forms such as broadcast media, the Court held that it was unlikely for users to have involuntary access to pornographic material online.[40] Therefore, the government could not justify the broad criminalization of pornography transmission and receipt where less restrictive alternative means were readily available.[41] The Supreme Court noted, however, that the holding did not apply to obscene speech, which enjoys no First Amendment protection and can be banned completely.[42] The Court drew a distinction between the terms used and stated "[T]he restriction of "obscene" material enjoys a textual manifestation separate from that for 'indecent' material, which we have held unconstitutional."[43] The Court therefore severed the term "or indecent" from section 223(a) and left the remaining text intact.[44]

The distinction drawn between what is indecent and what constitutes obscene unprotected speech did nothing to help victims of non-consensual Internet pornography. Obscene pornography under the *Miller* test is defined as pornography which an average person would feel appeals to prurient interests, depicts or describes sexual conduct in a patently offensive way, and lacks serious literary, artistic, political, or scientific value.[45] The average revenge pornography would unlikely meet the second prong of the *Miller* test. Since revenge porn usually includes nude photographs or consensual sex between lovers, generally it is not considered to be patently offensive. Such pornography may not even pass the first prong if the vengeful material consists of partial nudity or sexual acts that bear no resemblance to the graphic and elaborate videos and images to which most pornography viewers have grown accustomed. As for the third prong, unfortunately the widely accepted

38. *Id.*

39. Miller v. California, 413 U.S. 15, 24 (1973).

40. *Reno*, 521 U.S. at 869–70.

41. *Id.* at 854.

42. *Id.* at 883.

43. *Id.* at 868.

44. *Id.*

45. *See* Miller v. California, 413 U.S. 15, 24 (1973).

commercialization of the porn industry brought pornography within the context of copyright protection, which has traditionally been awarded only to useful art and science. Bringing pornography into the copyright arena clearly means that such works can possess artistic value, whether as a form of choreographic, audiovisual or pictorial works, or other artistic forms of expression.[46] While the First Amendment only protects pornography if it is not obscene, copyright law is even more pornography-friendly as it protects such material even if it is deemed obscene.[47]

In 1979, a federal judge concluded that pornographic films were entitled to copyright protection; since then, copyright law has played an important part in making pornography a work of art that has been accepted into mainstream American culture.[48] The Fifth Circuit has held that holding obscene materials copyrightable furthered the purposes of the Copyright Act to promote creativity, and of copyright power generally.[49] In 2004, a federal judge of the Southern District of New York came to a similar conclusion.[50] Like the Fifth Circuit, Judge Baer did not consider any social or moral reasons and argued that obscene materials were never intended to be given copyright protection, which is why obscene works were not copyrightable from the time the first U.S. copyright law took effect in 1790 up until the *Mitchell Brothers* decision, almost two hundred years later.[51]

With the grant of First Amendment protection to the Internet, similar to that enjoyed by print media, only a limited class of speech remains unprotected.[52] This includes speech that involves: obscenity, defamation, fraud, incitement, true threats, and speech integral to criminal conduct.[53] Therefore legal claims often rely on tort actions and remedies.[54] Such claims do not sufficiently compensate victims because the injury caused is impossible to retract; once the damaging images become a part of the World Wide Web, and the victim suffers every time someone gains access to the material. Furthermore, protection afforded to service providers has restricted civil claims to the actual ex-lovers and those responsible for initially transmitting the

46. *See generally* 17 U.S.C. § 102.

47. Bartow, *supra* note 15, at 831.

48. *See* Mitchell Bros. Film Group v. Cinema Adult Theater, 604 F.2d 852, 854 (5th Cir. 1979).

49. *Id.* at 856–57.

50. Nova Prods., Inc. v. Kisma Video, Inc., 02 Civ. 3850 (HB), 2004 U.S. Dist. LEXIS 24171, at *10–11(S.D.N.Y. Nov. 30, 2004).

51. Bartow, *supra* note 15, at 833.

52. *See generally* Huppin, *supra* note 21.

53. *Id.* at 48.

54. Jacqueline D. Lipton, *Combating Cyber-Victimization*, 26 BERKLEY TECH. L.J. 1103, 1107 (2011).

images onto the Internet.[55] It is unlikely that defendants have gained any financial benefits from the images and do not have deep pockets to ensure any adequate restitution.[56]

Although the notion of banning pornography altogether to protect potential victimization has not seen any success historically, the issue has not been altogether abandoned by our legal culture. The ever-prevalent fear faced by those who have ever self-generated sexually implicit material, combined with the possibility of grave danger to the reputation, careers, and physical well-being of potential victims, has brought about criminal statutes aimed at cyber-harassment and cyber-stalking.

B. The Laws Leading to Internet Service Provider (ISP) Absolute Immunity for Libel

The first Internet libel case litigated in the United States came in 1991, where the Southern District of New York held that an ISP was not liable for hosting defamatory content unless it was a "publisher" as opposed to a mere "distributor."[57] In *Cubby Inc. v. CompuServe Inc.*, the defendant ISP, CompuServe, provided CompuServe Information Service (CIS) among its other products and services.[58] CIS was an electronic library that gave subscribers access to thousands of information sources, bulletin boards, databases, and interactive online conferences.[59] One of the available forums was a Journalism forum, and CompuServe hired an independent company, CIS, to monitor the content of the Journalism forum in accordance with CompuServe's editorial and technical standards and conventions of style.[60] "Rumorville USA" was a publication available on the forum, which was owned and operated by a third party that had no affiliation with CompuServe other than its subscription to CompuServe's forums.[61] Plaintiffs were owners of a database that published and distributed news and gossip.[62] A claim arose when Rumorville published allegedly defamatory remarks relating to plaintiffs and their database.[63] Because the defamatory statements were published on CompuServe's Journalism forum, plaintiffs sued the company for publishing the

55. *Id.*

56. *Id.* at 1131.

57. Scott Sterling, *International Law of Mystery: Holding Internet Service Providers Liable for Defamation and the Needs for a Comprehensive International Solution*, 21 LOY. L.A. ENT. L. REV. 327, 332–33 (2001).

58. Cubby Inc. v. CompuServe, 776 F. Supp. 135, 137 (S.D.N.Y. 1991).

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.* at 138.

63. *Id.*

material and for failing to remove it from its forum.[64] The Court held that because the Rumorville USA operator directly uploaded the defaming content on the forum, defendant ISP had minimal editorial control over the publishing process, and therefore was not responsible for monitoring everything that was published onto its websites.[65] The ISP was hence not liable for mere distribution where it neither knew nor had reason to know of the defamatory statements.[66]

In 1995, *Stratton Oakmont Inc., v. Prodigy Services Co.* changed the law's previous stance and held that the defendant ISP was a publisher of defamatory statements posted on its public online forum.[67] The *Stratton* court distinguished the case from *Cubby* because the defendant in *Stratton* held itself out to be a "family-oriented service" by claiming that it had editorial control over the content posted on its bulletin board because it utilized an automatic software-screening program to filter the content.[68] The result of *Stratton* was that an ISP was not liable for any defamatory content published on its websites as long as it did not attempt to monitor the material published and exercise editorial control.[69] Because monitoring data available on the Internet was a service to society, especially parents who sought to resist their children's access to inappropriate material on the Internet, the *Stratton* holding did not last very long.[70]

Congress enacted the Communications Decency Act of 1996 (CDA)[71] to protect minors from harmful material on the Internet,[72] and to grant criminal and civil immunity to those providers of such harmful content as long as they attempt to restrict underage access.[73] CDA criminalizes the "knowing" transmission of "obscene or indecent" messages to any recipient less than 18 years of age.[74] Patently offensive material includes any message "that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs."[75]

64. *Cubby, Inc.*, 776 F. Supp. at 138.

65. *Id.* at 140.

66. *Id.* at 141.

67. *See* Stratton Oakmont Inc. v. Prodigy Services Co. Stratton Oakmont Inc. v. Prodigy Services Co. No. 31063/94, 1995 N.Y. Misc. LEXIS 229, at *10 (1995); *see also* Sterling, *supra* note 57, at 333.

68. *Stratton*, 1995 N.Y. Misc. LEXIS 229, at *10.

69. *Id.*

70. Sterling, *supra* note 57, at 336.

71. 47 U.S.C. § 230 (1996).

72. *Id.* § 230(b)(4).

73. *Id.* § 230(c).

74. *Id.* § 223(a).

75. *Id.*

Affirmative defenses are provided for those who take "good faith, . . . effective . . . actions" to restrict access by minors to the prohibited communications and those who restrict such access by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number.[76] The Act failed to define the terms "indecent" and "patently offensive" which brought on criticism attacking it forf being too vague and thereby violating the Fifth Amendment.

Because the CDA imposed a duty on information providers to restrict underage access, monitoring content of published material and exercising editorial control was necessary for the Act to succeed.[77] Therefore, the CDA overruled *Stratton* and allowed ISPs to maintain editorial control of their sites while escaping any "publisher's liability."

Ultimately in 1997, the Supreme Court in *Zeran v. America Online, Inc.* explicitly abolished the distinction between "publisher" and "distributor" that was first presented in *Cubby* and held that an ISP was not liable for material uploaded onto its website regardless of whether hosting the material categorized the ISP as a publisher or a distributer.[78]

III. Current State of the Law

Revenge pornography is sexually graphic images of individuals distributed over the Internet without the subject's consent, for the purpose of humiliating or harassing such individuals.[79] The distributors are more often than not ex-lovers angered by bad break-ups.[80] These images may be originally obtained without consent (e.g. hidden recordings of nudity and sexual conduct or through non-consensual searches of cell phones and private computers), or may be obtained with consent given within the context of an intimate relationship.[81]

A. ISP's Liability

Section 230(c) of the CDA states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[82] Under the Act, service providers of revenge porn are immune from any liability for distribution of non-consensual sexual material provided by a third-party

76. *Id.* § 223(e)(5)(A).

77. Sterling, *supra* note 58, at 336.

78. Zeran v. America Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997).

79. Chris Picazo, *Bill Would Criminalize Distribution of Non-Consensual Sexting*, Badger Herald (Oct. 15, 2013), http://badgerherald.com/news/2013/10/15/bill-criminalize-non-consensual-sexting/#.UvPmvf3rH0g.

80. *Id.*

81. Ann Bartow, *Copyright Law and Pornography*, 91 Or. L. Rev. 3, 44 (2012).

82. 47 U.S.C. § 230(c)(1996).

user.[83] The difference between service providers and information content providers can be illustrated by the decision of the Ninth Circuit Court of Appeals that refused to apply the CDA immunity clause to the website Roommates.com in a claim of violation of the Fair Housing Act (FHA).[84] The website asked users a series of questions, including inquiries about sexual orientation, family status, and roommate's sex preference.[85] The information gathered was then used to ensure that only those who met the desired criteria could view the listings.[86] This act of filtering listings by personal preferences to match roommates was a violation of FHA because it limited housing options based on discriminatory factors.[87] The court held that Roommates.com was not merely a service provider since it was responsible for creating the questions and filtering results, thereby partaking in providing the discriminatory content of information.[88] Under this analysis, most websites, including "MyEx.com," clearly foresee that most information on their site will be non-consensual in nature, enjoy CDA immunity as long as all they do is provide space for vengeful posts, such as offensive texts, images and videos, and do not actively participate in forming the content themselves.

In *Barnes v. Yahoo! Inc.*, the Oregon District Court heard a case in which Cecilia Barnes was harassed and stalked by a number of men who had viewed her online profile, which included her name, workplace contact information, and nude photographs.[89] Barnes was unaware of the profile until the men showed up at her work after viewing the profile on a web page hosted by Yahoo! Inc.[90] It was then that she discovered an ex-boyfriend created her online persona.[91] Barnes informed Yahoo that she had not consented to the online display of her nude photographs but the company did not remove the profile.[92] The district court held that Yahoo was not liable for the unauthorized exhibit of her private photographs and contact information because it was merely a service provider.[93] The Ninth Circuit later found that Barnes had a cause of action against the company because a Yahoo representative had promised to remove the photographs upon Barnes request, but failed to

83. Bartow, *Copyright Law and Pornography*, *supra* note 81, at 24.

84. Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1175–76 (2008).

85. *Id.* at 1161.

86. *Id.* at 1162.

87. *Id.*

88. *Id.* at 1172.

89. Barnes v. Yahoo!, Inc., No. 05-926-AA, 2005 U.S. Dist. LEXIS 28061, at *1 (D. Or. Nov. 8, 2005).

90. *Id.* at *2.

91. *Id.*

92. *Id.* at *3.

93. *Id.* at *10.

honor that promise.[94] This decision demonstrates that website hosts are not liable for any damages caused as long as they avoid making any promises to the victim.

Before 1979, pornography was unable to gain protection under copyright laws and therefore did not have the economic incentive of being sole beneficiaries of their work. But then, in *Mitchell Brothers Film Group v. Cinema Adult Theater*, the Fifth Circuit held that obscenity was not a defense to copyright infringement because the language of the Copyright Act of 1909 did not preclude the copyrighting of obscene material.[95] On October 28, 1998, President Bill Clinton signed the Digital Millennium Copyright Act (DMCA)[96] into lawr to protect copyright holders against the growing threat of infringement brought on by the widespread use of the Internet.[97] The Act criminalized actions that "circumvent a technology measure that effectively controls access to a copyrighted work."[98] The DMCA bars the production or dissemination of technology that allows users to circumvent digital copyright protection.[99] The sanctions for violation of the Act include a fine of up to $500,000 or imprisonment of up to five years.[100] The immunity granted to service providers under the CDA does not preclude liability under intellectual property law. However, the Online Copyright Infringement Liability Limitation Act (OCILLA), a part of the DMCA, provides for some liability to service providers; under OCILLA, if a service provider is put on notice that it is hosting protected copyright material, he must remove such material to escape copyright infringement charges.[101]

Once again, website providers are given the opportunity to gain immunity from copyright infringements. Service providers are not required to determine whether an image or information is copyright-protected before making third-party posts visible on their web pages, they are only required to remove such material when someone complains of a copyright infringement and has a valid copyright. The problem then remains for victims of revenge porn, who are often uneligible for copyright protection of amateur self-productions of sexual images. Even when the images could somehow qualify as art capable of such protection, the person actually taking the photos or producing the videos gets the copyright, which may have been the scornful ex-

94. Barnes v. Yahoo!, Inc., 565 F.3d 560, 562 (9th Cir. 2009).

95. Mitchell Bros. Film Group v. Cinema Adult Theater, 604 F.2d 852, 854 (5th Cir. 1979).

96. Digital Millennium Copyright Act, 1998, Enacted H.R. 2281, 105 Enacted H.R. 2281, 112 Stat. 2860.

97. Ronneburger, *supra* note 16, at 24.

98. *Id.*

99. *Id.*

100. *Id.*

101. *Id.* at 25.

lover. Even if the victim were able to obtain a copyright for his or her nude images, by the time he or she would learn of the presence of the images on the web and inform the service providers of the infringement, it would be too late. Once the image is made available on the Internet, it is forever accessible across the globe.

B. Publisher's Liability

Revenge porn offenses are normally prosecuted under tort laws.[102] These include claims of defamation, privacy torts, and intentional infliction of emotional distress.

i. Tort Liability

a. Defamation

A claim for defamation requires:

> (1) a false and defamatory statement concerning another; (2) an unprivileged publication to a third party; (3) fault amounting at least to negligence on the part of the publisher; and (4) either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication.[103]

The foundation of defamation laws is a person's right to an unimpaired reputation.[104] Defaming one's reputation exposes a person to hatred, contempt, ridicule, or obloquy, causes that person to be shunned or avoided, or has a tendency to injure that person in his or her occupation.[105]

b. Privacy Torts

Privacy torts include (1) intrusion into seclusion; (2) public disclosure of private facts; (3) false light publicity; and (4) commercial misappropriation of name or likeness.[106] Invasion of privacy and defamation are two separate torts that focus on a similar harm-causing action.[107] To succeed in a claim for false right, a plaintiff must show that the defendant, with knowledge of falsity or in reckless disregard of the truth, placed the plaintiff before the public in a false position that would have been highly offensive to a reasonable person.[108]

---

102. *See generally id.* at 3.

103. RESTATEMENT (SECOND) OF TORTS § 558 (1977).

104. 11 FRUMER & FRIEDMAN, PERSONAL INJURY ACTIONS, DEFENSES, AND DAMAGES § 46.01[2] (Matthew Bender, Rev. Ed.).

105. *Id.*

106. RESTATEMENT (SECOND) OF TORTS §§ 652[B]–[D] (1977).

107. *Id.* § 46.01[d].

108. *Id.* § 652E.

c. Intentional Infliction of Emotional Distress[109]

There are various challenges to these tort claims. One challenge that is common to all three claims is that the anonymous nature of Internet postings permits the perpetrator to hide his identity using pseudonyms or utilizing public computers.[110] It is not impossible to decipher the identity of the anonymous distributor, but by the time that identity becomes known it is too late to contain the damage.[111] In addition to the urgency of unmasking the offender, money and resources are a concern.[112] While costs of criminal charges are borne by the State, seeking tort damages requires money. Not only does the victim have to initially come up with court and attorney's fees, attempts to circumvent a distributor's anonymity often require court orders, which require more time and money.[113] Finally, litigation draws more attention to the issue and subjects the victim to more humiliation and harassment.[114]

ii. Liability under Civil Rights Law

Another avenue for obtaining some relief for victims of revenge porn is a suit alleging gender discrimination. The Civil Rights Act of 1964 prohibits gender discrimination as a result of intimidation, threats, or coercion aimed at interfering with employment opportunities.[115]

iii. Criminal Liability Under State Laws

Whereas people with insufficient funds are unlikely to be deterred by the threat of tort-based claims since they have limited resources to protect, criminal sanctions could help deter such potential offenders. In 2004, New Jersey became the first state to criminalize revenge porn.[116] The law in New Jersey makes it a felony for a person to distribute sexually explicit photographs and films of an individual when they know they do not have the subject's consent.[117] The law states:

> An actor commits a crime of the third degree if, knowing that he is not licensed or privileged to do so, he discloses any photograph,

109. *Id.* § 46 ("One who by extreme or outrageous conduct intentionally or recklessly cause severe emotional distress to another is subject to liability for such emotional distress, and if bodily harm to the other results from it, for such bodily harm.").

110. Lipton, *supra* note 54, at 1129.

111. *Id.* at 1129–30.

112. *Id.*

113. *Id.*

114. *Id.*

115. *Id.* at 1138; *see* 18 U.S.C. § 245(b) (2006).

116. N.J. STAT. ANN. § 2C: 14-9 (West 2004).

117. *Id.* § 2C: 14-9(c).

> film, videotape, recording or any other reproduction of the image of another person whose intimate parts are exposed or who engaged in an act of sexual penetration or sexual contact, unless that person has consented to such disclosure. For purposes of this subsection, "disclose" means sell, manufacture, give, provide, lend, trade, mail, deliver, transfer, publish, distribute, circulate, disseminate, present, exhibit, advertise or offer.[118]

In 2012, Dharun Ravi, a student of Rutgers University, distributed webcam footage of his roommate Tyler Clamenti engaging in sexual activity with another man.[119] The distribution caused Clamenti to commit suicide by jumping off of New York City's George Washington Bridge.[120] Ravi faced a possible maximum sentence of ten years in prison, but was instead sentenced to 30 days in jail,[121] three years of probation, 300 hours of community service, attendance of a cyber bullying counseling program, and a $10,000 fine to be paid to the New Jersey probation department for programs that assist people who are victims of bias crimes.[122] In October 2013, California legislature adopted the Revenge Porn Act, and added subsection (j)(4) to the California penal code.[123] The law states:

> Any person who photographs or records by any means the image of the intimate body part or parts of another identifiable person, under circumstances where the parties agree or understand that the image shall remain private, and the person subsequently distributes the image taken, with the intent to cause serious emotional distress, and the depicted person suffers serious emotional distress.[124]

This law specifically targets ex-lovers and spouses who distribute video and images on revenge porn websites with the intent to humiliate or harass their victims.[125] In November 2013, the state assembly of Wisconsin overwhelmingly passed the Republican proposal to outlaw the posting of revenge

118. *Id.*

119. Megan DiMarco & Alexi Friedman, *Live Blog: Dharun Ravi Sentenced to 30 Days in Jail*, STAR-LEDGER (May 21, 2012), http://www.nj.com/news/index.ssf/2012/05/dharun_ravi_sentenced_for_bias.html; *see also* State v. Ravi, No. 11-04-00596, 2012 N.J. Super. LEXIS 1757, at *1 (App. Div. May 21, 2012).

120. DiMarco & Friedman, *supra* note 119.

121. *Ravi*, 2012 N.J. Super. Unpub. LEXIS 1757, at *1.

122. DiMarco & Friedman, *supra* note 119.

123. CAL. PENAL CODE § 647(j)(4) (as amended, effective Oct. 1, 2013).

124. *Id.* § 647(j)(4)(A).

125. Picazo, *supra* note 79.

porn on the Internet.[126] Representative John Spiros was responsible for circulating the bill that proposed to criminalize the non-consensual distribution of sexually explicit material.[127] Katherine Bates, spokesperson for Spiros, said:

> Times have changed, the proliferation of cell phones with cameras and video capabilities makes this legislation pertinent to protect a generation who are a point and click away from having their private moments made public. People have lost their jobs and have committed suicide. People have had to change their names because they have been stalked. People's lives have been ruined. Their rights are not protected.[128]

According to Bates, "[t]he bill would update the current law to reflect new, emerging technology."[129] Passing this Bill would make Wisconsin the third state to criminalize revenge pornography; and Arizona, Florida, Illinois, Maryland, and New York may soon follow suit as they have begun considering the adoption of similar revenge porn laws.[130]

iv. Liability Under Federal Laws

Criminalizing stalking and harassment is not a new phenomenon. There are various federal criminal statutes that could potentially be used in bringing down unauthorized porn distributors, though victims have not gained much success under them because federal legislation is not very consistent when applied to online abuses.[131]

a. Interstate Communications Act

The Interstate Communications Act provides that "whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both."[132] This provision is often ineffective in restricting online abuse because it requires a

126. Todd Richmond, *Bill Banning 'Revenge Porn' Passes Wisconsin Assembly Overwhelmingly*, CHI. SUN-TIMES (Nov. 12, 2013), http://www.suntimes.com/news/nation/23719333-418/bill-banning-revenge-porn-passes-wisconsin-assembly-overwhelmingly.html.

127. Picazo, *supra* note 79.

128. *Id.*

129. *Id.*

130. Katy Steinmetz, *A New Strategy for Prosecuting Revenge Porn: California's Attorney General Avoids the State's Revenge-Porn Law in a New Indictment*, TIME U.S. (Dec. 10, 2013), http://nation.time.com/2013/12/10/a-new-strategy-for-prosecuting-revenge-porn/#ixzz2vIkS64CL.

131. *See* Lipton, *supra* note 54, at 1118.

132. 18 U.S.C. § 875(c) (2006).

threat of physical injury, which revenge pornography does not cause unless it leads to sexual assault that would not have occurred but for the criminal post, and even then physical harm may not be the intent of the poster.[133] Revenge pornography is not specifically directed at the victims; instead it is about the targeted victims on generally accessible websites.[134] Therefore, the Interstate Communications Act does not cover situations where an ex-lover impersonates the victim online to incite third parties to harass or harm the victim, as was the case in Barnes.[135]

b. Telephone Harassment Act

The federal Telephone Harassment Act could pertain to online harassment.[136] The Statute was revised in 2006 to prohibit a person from making a telephone call or utilizing a communications device without disclosing his or her identity and "with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications."[137] The purpose of the revisions was to capture harassing e-mails.[138] This Statute, like the Interstate Communications Act, requires that the harassment be directed at the victim for it to be actionable.[139] The simple posting of harassment-inducing material online, as is the case with revenge pornography, will not result in a cause of action under this Act.[140] Furthermore, because most revenge pornography is posted anonymously, the prohibition will not apply as the Statute contains the element that the offender must have failed to disclose his identity and the victim cannot otherwise have gained knowledge of his identity.[141]

c. Interstate Stalking Punishment and Prevention Act (FISPPA)

At first, FISPAA only criminalized harassing behavior with the intent to kill or cause serious bodily harm to a person, itslanguage was modified by the Violence Against Women Act in 2006 to include the same criminal penalties where the behavior is intended not only to kill or cause bodily harm,

133. Lipton, *supra* note 54, at 1118.

134. *Id.*

135. *Id.*; *see* Barnes v. Yahoo!, Inc., No. 05-926-AA, 2005 U.S. Dist. LEXIS 28061, at *2 (D. Or. Nov. 8, 2005).

136. Lipton, *supra* note 54, at 1118.

137. 47 U.S.C. § 223(a)(1)(C) (2006).

138. Lipton, *supra* note 54, at 1118–19.

139. *Id.*

140. *Id.*

141. *Id.*

but also simply to harass.[142] But criminal sanctions are usually given out only to those who are persistent in their acts of posting damaging information and images because an isolated act usually does not rise to the level of harassment or a reasonable threat.[143] The Federal Cyber-stalking Statute makes it a felony to use any "interactive computer service" to engage in a "course of conduct" that is intended to harass or intimidate someone in another state and either places that person in reasonable fear of serious bodily injury or death or that would reasonably be expected to cause the person to suffer "substantial emotional distress."[144] Nearly all states have enacted similar cyber-stalking and harassment statutes, but most states treat the offenses as misdemeanors that result in little or no jail time.[145] It is unlikely for any victim to prove that website operators had the intent to harass, even if their website is designed for the purpose of posting harassing materials. Since the website does have actual knowledge that the distributions are non-consensual at the time they are posted, they are later immune from civil liability.

FISPPA prohibits harassment and intimidation in "interstate or foreign commerce" and has been amended to include conduct that utilizes "the mail, any interactive computer services, or any facility of interstate or foreign commerce to engage in a course of conduct that causes substantial emotional distress."[146] Fortunately, FSPPA does not have the specific direction of communication limitation found in the previously discussed federal statutes.[147] The direction of the conduct is not the focus of the Statute, but rather it is the act of utilizing an interactive computer service to cause emotional distress upon the victim.[148]

d. Computer Fraud and Abuse Act (CFAA)

CFAA was enacted to deal with the unauthorized hacking of computer systems.[149] CFAA punishments are only accessible to victims of revenge por-

142. Federal Interstate Stalking Punishment and Prevention Act, 18 U.S.C. § 2261A (2006), amended by Violence Against Women and Department of Justice Reauthorization Act of 2005, 119 Stat. 2960, 2987–88 (2006).

143. Ellen Luu, Note, *Web-Assited Suicide and the First Amendment*, 36 HASTINGS CONST. L. Q. 307, 322–23 (2009).

144. 18 U.S.C. § 2261A (2006).

145. Joseph C. Merchman, Note, *The Dark Side of the Web: Cyberstalking and the Need For Contemporary Legislation*, 24 HARV. WOMEN'S L.J. 255, 257 (2001).

146. Lipton, *supra* 54, at 1119 (citing 18. U.S.C. 2261A(1), (2) (2006).

147. *Id.*

148. Lipton, *supra* note 54, at 1120.

149. *Id.*

nography where the perpetrator has gained access to the pornographic images via unauthorized trespass into a private computer.[150]

e. Extortion

California attorney general Kamala Harris recently charged a 27-year-old man with identity theft and extortion for running a revenge porn website.[151] The charge involved a San Diego resident, Kevin Bollaert, who allegedly ran the website "ugotposted.com." The site was set up to host pictures, as well as information about the subjects including links to Facebook profiles.[152] Allegedly, Bollaert ran a sister website called "changeyourreputation.com," which offered to make the images disappear for around $300.[153] Notice how this enterprise is similar to MyEx.com. It is common practice to find reputation-protection services offered alongside websites that are responsible for damaging reputations in the first place.[154] Victims of the postings reported that they were hounded by messages and phone calls after the photographs were posted.[155] People found the contact information from the corresponding Facebook links and began harassing the subjects of the images.[156] One victim wrote an email to the site administrator expressing her fear and distress, but the photos were not removed.[157] In her email, the victim stated that she was "scared for her life" because "People are calling my work place and they obtained the information from this site![158] Her email continued, "I have contacted the police but these pictures need to come down! Please!"[159] Apparently, her threat to contact police was not enough to motivate the website operator to take any action in spite of the victim's desperate request.[160] Perhaps the law granting immunity to service providers has created such confidence among website operators that they fail to consider the creative ways law enforcement officials have begun using it to bring about justice.

---

150. *Id.*; for an example of such a hacking, see *infra* part I (indictment of Hunter, Moore and Charles Evans).

151. Steinmetz, *supra* note 130.

152. *Id.*

153. *Id.*

154. *Id.*

155. *Id.*

156. *Id.*

157. Steinmetz, *supra* note 130.

158. *Id.*

159. *Id.*

160. *Id.*

C. Liability Under Foreign Laws

i. ISP's Liability

a. China

In China, the right to one's reputation is fundamental, and it is specifically stated in the Chinese Constitution.[161] Article 101 of the General Principles of the Civil Law of the People's Republic of China (GPCL) also recognizes the invaluable nature of this right by stating "[t]he personality of citizens shall be protected by law, and the use of insults, libel or other means to damage the reputation of citizens or legal persons shall be prohibited."[162] Law enforcement officers have the authority to detain a person for up to ten days for merely insulting someone.[163] Naturally then China gives the right of reputation the same weight as freedom of speech, if not more. ISPs in China must cease the transmission of any insulting or defamatory remarks, maintain personal records, and report the distribution of such information to the relevant authorities.[164]

In *Gao Xiaosong v. Yahoo!(Holdings) Hong Kong Ltd.*, the Beijing Court of China held Yahoo China liable even though it removed all defamatory content that pertained to plaintiff's reputation before trial commenced and it published the plaintiff's statements in an attempt to redress the harm.[165] In *Gao Xiaosong*, a print media company published defamatory information that plaintiff was a "mean employer" and that he threatened his manager, along with other reports of Gao's involvement in the suicide of a pop singer.[166] Because the clippings of the media reports were made available on Yahoo China, owned by defendant, Gao sued it along with his manager and the media organization.[167]

b. United Kingdom (UK)

ISPs in UK are not absolutely immune from liability for hosting defamatory content. Before 1996, ISP liability depended on the category of service providers to which the ISP belonged.[168] These categories included publishers, printers, distributors, and vendors.[169] In 1996, the law changed and ISPs were

161. XIANFA art. 101, § VI (1986) (P.R.C.).

162. *Id.*

163. Anne S.Y. Cheung, *A Study of Cyber Violence and Internet Service Provider's Liability: Lessons from China*, 18 PAC. RIM L. & POL'Y J. 323, 326 (2009).

164. *Id.* at 328.

165. *Id.* at 330.

166. *Id.*

167. *Id.*

168. Sterling, *supra* note 57, at 338.

169. *Id.*

generally held liable for the content they hosted.[170] The only recourse available to these service providers was a successful invocation of the "Innocent Disseminator" defense.[171] To succeed in defending a defamatory posting claim under the United Kingdom Defamation Act of 1996, an ISP had to negate a showing that notice of the defamatory nature of the content displayed on its website was never received.[172] The three-pronged defense available under the act allowed an ISP to avoid liability if it is not (1) the author, editor or publisher of the defamatory content; (2) exercised reasonable care in its operations; and (3) can show that it did not know, nor had any reason to believe, that it caused or contributed to the distribution of such material.[173] *Godfrey v. Demon Internet Ltd.* held that even though defendant ISP was not a publisher of the defamatory material, it could not evade liability because it failed to prove all the elements of the defense.[174] Because the defendant was given notice of the defamatory nature of the content available on its server, the ISP was liable for defamation.[175] Therefore, as long as a plaintiff could prove that the posting of an unknown third party was defamatory and that notice of this nature of the post had been communicated to the ISP, the ISP would be held liable.

In 2002, UK became bound by the European Union (EU) standard under the Electronic Commerce Regulation of 2002 (EC Directive).[176] The EC Directive establishes legal rules that online retailers and service providers must comply with when dealing with consumers in the twenty-seven member countries of EU and lays out the circumstances under which an ISP should be held accountable for material that they host, cache, or carry but did not create, meaning that they were mere conduits and therefore will be entitled a safe haven.[177] The directive specifies that ISPs do not have an affirmative duty to monitor information hosted on their websites.[178] In *Bunt v. Tilley*, the court made a decision based on both the *Godfrey* holding and the EC Directive, and found that an ISP can only be held liable for defamatory publica-

170. *See* Defamation Act, 1996, c. 31, § 1(1) (Eng.).

171. Cheung, *supra* note 163, at 341.

172. *See generally* Defamation Act, c. 31, § 1(1).

173. Sterling, *supra* note 58, at 339.

174. 1999 E.M.L.R. 542 (Q.B.) (Eng.); Sterling *supra* note 58, at 340.

175. Sterling, *supra* note 57, at 340.

176. The Electronic Commerce (EC Directive) Regulations, S.I. 2002/2013 (UK.) (implementing the Council Directive on Electronic Commerce), 2000/31/EC, art. 14, 2000 O.J. (L 178/1)(EC), *available at* http://www.opsi.gov.uk/si/si2002/20022013.htm.

177. Cheung, *supra* note 163, at 342.

178. *Id.*

tions if it was a "knowing participant."[179] Because a passive role of the ISP is no longer enough to incur liability, a plaintiff must give actual notice to the defendant ISP.[180] The case thereby eliminated the effectiveness of the Defamation Act's provision that required that the ISP have no reason to know of its participation in distributing defamatory content. Only actual notice suffices in bringing down an ISP in a claim for defamation on the Internet.

c. Australia

Australian courts have not seen much litigation over ISP liability under defamation laws.[181] The case before court that involved a claim against a defendant who failed to remove defamatory posters from his property has been analogized as capable of being applied to ISPs.[182] In *Urbanchich v. Drummoyne Municipal Council*, the court held that the defendant, by failing to remove the illicit material from his property, became a publisher of the material and was liable for damages.[183]

Australian statutory law pertaining to ISP liability for defamation is similar to that of UK. The law in Australia holds an ISP liable unless it can prove that (1) it did not have knowledge of the defamatory nature of the material; (2) it did not know that the material was likely to be defamatory; and (3) this lack of knowledge was not due to the ISP's negligence.[184]

d. Japan

Japan enacted the Provider Liability Limitations Act in 2002.[185] The law covers copyright violation, defamation, and obscenity among other things. Regarding those contents that have to be removed, the law holds that the service providers cannot be held liable unless (1) they have the technological means to remove the content and (2) they (a) have the knowledge of the illegal content, or (b) they could reasonably have gotten to know it.[186] It also specifies circumstances under which service providers may offer personal

179. *See id.*; Bunt v. Tilley, (2006) EWHC 407 (QB), *available at* http://www.bailii.org/ew/cases/EWHC/QB/2006/407.html.

180. *Bunt*, (2006) EWHC 407 (QB), *available at* http://www.bailii.org/ew/cases/EWHC/QB/2006/407.html.

181. Sterling, *supra* 57, at 342.

182. *Id.*

183. *Id.*; *see* 1988 N.S.W. LEXIS 8802 (N.S.W. Austl. Dec. 22, 1988).

184. Sterling, *supra* note 57, at 343.

185. Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders ("Providers Liability Limitation Act") No. 137 (2001) (effective May 27, 2002).

186. *See generally id.*

information of a user to another.[187] In addition, an Internet industry association of software development and Internet companies, the Electronic Network Consortium, has drafted guidelines that require that Internet use be conducted in appropriate manners.[188] In *Niftyserve*, the plaintiff sued a Japanese online service for its failure to remove an offensive statement posted by a third party from its website.[189] Niftyserve, the defendant, had hired a company to monitor the content of its website, but failed to do so.[190] The Tokyo District court held that defendant ISP was liable for defamation under the principle of vicarious liability.[191]

e. Singapore

Singapore places strict liability on ISPs for hosting defamatory content.[192] The Class Scheme Action (CLS) was enacted in 1996.[193] Under this Act, all Singapore based ISPs must register with the Singapore Broadcasting Authority (SBA).[194] Additionally, the CLS stipulates that upon SBA's request, ISPs must deliver all of its records of services.[195] Finally, the CLS mandates that when directed by SBA, an ISP must remove all material that is deemed offensive or against public interest.[196]

ii. Poster's Criminal Liability

Certain foreign countries have dealt with revenge porn issues by enacting broad privacy statutes that may be applicable to revenge porn. In January 2014, Israel became the first country in the world to enact a nationwide law criminalizing revenge pornography.[197] The law makes putting a sex tape online without the consent of all the involved parties punishable by up to five years in prison.[198] This revenge pornography law, unlike the ones in New Jersey and California, criminalizes the act of posting such material by label-

187. *Id.*

188. Sterling, *supra* note 57, at 341.

189. *Id.* at 341–42.

190. *Id.*

191. *Id.*

192. *Id.* at 344.

193. *Id.*

194. Sterling, *supra* note 57, at 344.

195. *Id.*

196. *Id.*

197. Sam Frizell, *Israel Bans 'Revenge Porn'*, TIME WORLD (Jan. 7, 2014), http://world.time.com/2014/01/07/israel-bans-revenge-porn.

198. *Id.*

ing it sexual assault.[199] Similar U.S. laws, however, criminalize the act as defamation and harassment. The Israeli law was drafted by MK Yifat Kariv (Yesh Atid) after a video of two people engaging in intercourse was posted on Whatsapp and viewed by 10,000 people.[200] The male participant in the video posted it in retaliation of his lover breaking up with him; the posting was punishable by up to 5 years in prison.[201]

France criminalizes the willful violation of the intimate private life of another by "transmitting the picture of a person who is within a private place, without the consent of the person concerned."[202] The Philippines' Anti Photo and Video Voyeurism Act of 2009 criminalizes copying, reproducing, sharing, or exhibiting sexually explicit images or videos over the Internet without written consent of the individual depicted.[203] The "Sexting" laws of the Australia state of Victoria makes it illegal to publish nude pictures of a person without his or her consent.[204]

Although the criminalization of revenge pornography has received global support, finding and prosecuting offenders is a daunting task due to various conflicts with federal law and constitutional guaranteed rights. There are multiple Fourth Amendment concerns involved when finding the offenders, who most often post anonymously.[205] Police officers can track IP addresses to find the culprits but they must have probable cause to conduct computer searches.[206] Additionally, most offenders can claim that their computer was hacked or left unattended.[207] Offenders could also post such criminalized material using public computers and leave no trace behind.

As this article has shown, service providers have been given First Amendment protection similar to the protection enjoyed by the print media; they do not have a duty to maintain records of a posting or release information. Even if the website providers can be charged with extortion, it is often

199. Tracey Wallace, *Israel Declares Revenge Porn Illegal, While America Still Drags Its Feet*, POLICYMIC (Jan. 22, 2014), http://www.policymic.com/articles/79693/israel-declares-revenge-porn-illegal-while-america-still-drags-its-feet.

200. *Id.*

201. *Id.*

202. CODE PENAL [C. PEN.] art. 226-1 (Fr.).

203. Philippines Anti-Photo and Video Voyeurism Act, No. 9995, 3rd Reg. Sess. (2010).

204. Jon Martindale, *Australian State Outlaws Revenge Porn*, KITGURU (Dec. 12, 2013), http://www.kitguru.net/channel/jon-martindale/australian-state-outlaws-revenge-porn.

205. *See generally* David Gray et al., *Symposium on Cybercrime: Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745, 797 (2013).

206. *Id.*

207. *Id.*

difficult, if not impossible, to find the actual operators because service providers can operate their websites from anywhere, including foreign countries, and fail to respond to any communication regarding the non-consensual material. Some websites can only be tracked to anonymous domain registrations, where "reputation protection services" payments are made to overseas accounts.[208]

IV. FORECAST/RECOMMENDATIONS

Having seen that our legal system remains inadequate, given the egregious nature of the consequences of revenge pornography and the lack of serious laws that deter the conduct, the following are current proposals which seek to provide greater protection to victims.

A. Revisions of Existing Criminal Legislation

Current Federal and State criminal statutes include elements such as "proximity" and "credible threat" that place a great burden of proof on the state.[209] As discussed above, these elements serve to ensure that freedom of speech rights are not curtailed in the process of protecting victims of cyber harassment. However, a balance between freedom of expression and protecting personal rights of reputation and privacy can be achieved without placing this undue burden. Instead of requiring a pattern of repetition to convict an offender, particularly harmful one-time occurrences should be punished with equal vigor.[210] Where one-time offenses of harassment via the telephone or mail may not cause much need for severe criminal sanctions, these one-time acts in the cyber world are far more damaging and egregious in nature.[211] Current laws that require repetitive conduct should be amended to state that repetitive conduct is *generally* required, so that judges have the discretion to punish single posts that are significantly appalling.[212] Current laws require that the harassing communication be sent directly to the victim. Direct communication requirements may have made sense when the injury sought to be remedied was physical in nature; however, in the realm of Internet harassment, the injury caused is much broader and includes physical, economic, emotional and psychological damage. Given the wide array of damages that are caused by an Internet post, which communicate to a vast number of people, such posts should be given at least the same weight as communication made directly to the victim.

The Megan Meir Cyber Bullying Prevention Act (MMCPA) was introduced in 2008 to combat the egregious consequences of cyber bullying, but

208. *See generally* Lipton, *supra* note 54.

209. *Id.*

210. *Id.* at 1127.

211. *Id.*

212. *Id.*

the law was never enacted.[213] The Act is named after the case *United States v. Drew*, where the defendant (Drew) escaped liability for cyber bullying that resulted in the death of thirteen-year-old Megan Meir.[214] Drew was the mother of one of Meir's classmates, and knew that Meir suffered with depression.[215] Drew bullied Meir by impersonating a fictional sixteen-year old boy, befriending the victim, and then later harassing her on MySpace.com.[216] Following Meir's suicide, the federal prosecutors charged Drew with a violation of the CFAA because Missouri law did not criminalize Drew's actions.[217] Drew evaded liability because the violation of a website's posted terms of service was not specifically addressed in CFAA.[218] The proposed law prohibited the transmission of communication "with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person; using electronic means to support severe, repeated, and hostile behavior."[219] An act similar to MMCPA could be drafted and would likely be approved as long as it successfully addresses First Amendment concerns.

Tackling First Amendment issues can be tricky since restricting vengeful pornographic posts deals with a form of speech the government has not sought to limit in the past. For example, in a child pornography case, the government was able to satisfy the strict scrutiny test of restricting speech by showing that the state's interest was compelling.[220] Revenge porn should be backed by an equally compelling interest. Protecting a victim's reputation may not justify imposing criminal sanctions for speech-related actions; however, prohibiting foreseeable physical and inevitable psychological harm may pass the threshold. If laws are targeted to prevent physical attacks on, and lifelong harm to reputation and well-being of, the victims of revenge pornography, it would be much harder to argue for First Amendment rights to take revenge.

Finally, criminal liability should be extended to users of such material. Punishing website users who access pornographic material would be a difficult task. The Supreme Court has held that adults have a right to view adult pornography, so any proposed legislation could attempt to only sanction repeat users of websites that clearly contain non-consensual material.[221] Because it is often difficult, if not impossible, to punish website sponsors who

213. *Id.* at 1121.

214. Lipton, *supra* note 54, at 1120. at 1120 (citing 259 F.R.D. 449 (C.D. Cal. 2009)).

215. *Id.*

216. *Id.*

217. *Id.* at 1121.

218. *Id.*

219. *Id.*

220. *See* Osborne v. Ohio, 495 U.S. 103, 109 (1990).

221. *See id.* at 137–40.

hide behind immunity or operate websites from foreign countries even after credible claims of their non-consensual content are made, it may be useful for the government to compile a list of websites that operate illegally by hosting non-consensual pornography. This list could then be distributed nationally through popular television channels, radio stations, and print media. Users of these websites who knowingly visit the websites repeatedly could then face possible criminal punishment. It may not be easy to prove that a user visited the website knowingly, given the issues with hacking and the hurdles of proving actual knowledge, but the law would act as a significant deterrent to website hosts and successfully limit the harm caused to victims. If less people risk visiting revenge porn websites, less damage would be caused to a victim's reputation.

B. Imposing Civil Liabilities on Web Service Providers

If website providers are treated like business owners, they may be subject to various tort liabilities. Website providers maintain control over the content of their websites, which may or may not be regarded as property.[222] Nevertheless, a provider of a web service is a person in possession because he or she maintains control of the occupants and content of the websites.[223] The duty of exercising reasonable care that tort law imposes on occupiers of land should likewise be applied to service providers. Some have suggested that just as home owners/tenants are required to take reasonable measures to control the conduct of inviteesand give them adequate warnings to avoid harm, website operators should be liable if they fail to exercise such precaution or give appropriate warnings.[224] Tort law has at times gone so far as to hold a property occupant liable for damages caused by third party crimes where the damages were foreseeable and likely to occur.[225] Because cyber-harassment is a crime, owners of websites such as MyEx.com should be held liable for the damages that result from cyber-harassment undertaken by ex-lovers of victims. An owner/creator of a website called MyEx.com surely foresees that cyber-harassment is likely to occur.

C. Mandatory Self-Regulating Requirements for Certain Web Site Sponsors

Requiring Internet service providers to continually monitor their sites for abuse may not be plausible, but perhaps the government could successfully impose certain requirements that a website sponsor must complete to take advantage of the service provider immunity. Given that pornography distribution is a heavily regulated industry, the government can regulate the

222. Nancy S. Kim, *Website Proprietorship and Online Harassment*, UTAH L. REV. 993, 1034 (2009).

223. *Id.* at 1036.

224. *Id.*

225. *Id.* at 1015.

industry without violating Fourth Amendment protections. Furthermore, heavy regulation of ISPs, similar to ISP regulations in Singapore, could not only bring ISPs out of the Fourth Amendment ban on governmental intrusion upon privacy, but the proposed regulations would also help law enforcement officials track the culprits. Heavily regulated activities and businesses find it more difficult to bring claims of Fourth Amendment violations as law enforcement's intrusion is justified due to the nature of the activity or business enterprise. If the following actions were mandated before a service provider could escape liability, instances of revenge pornography distribution could be drastically reduced.

i. Identifying the Posters

Website hosts could ask a user to register at the site before he or she can comment or post images. Use of the webpage would only be possible if the user listed a valid email address that is verified by clicking on a link sent by the website. This method of authenticating users is currently used by various web service providers. Although it is likely that a user may form an email address for the sole purpose of posting an ex lover's image, it will create an extra step to the process of uploading revenge pornography that many may not care to undergo. There is a possibility that given the strong hold of First Amendment rights, prohibiting anonymity may not satisfy the strict scrutiny analysis; in that case, the websites could include an anonymous posting option, but make the registered use the default option. Thus, when the user attempts to upload an image, he or she will be taken to a page to register unless a box is checked that says "post anonymously."[226] Alternatively, the user may be automatically taken to a user registration page with a "skip this step" option.

ii. Consent to Knowledge of Legal Consequences

When operating a website that features pornographic material, the website owner could be required to display a notice of the legal consequences for uploading non-consensual pornographic material, which a user must first agree to before entering the site.[227] A notice of legal ramifications will likely cause a first time poster of revenge pornography to think twice before uploading the damaging material.

iii. Indemnification Agreement

Users of such websites could be required to agree to indemnify the website owners for any lawsuits that result from unauthorized use of certain

226. *Id.* at 1017.

227. *Id.* at 1015.

materials.[228] Few people are likely to proceed once they realize that they are entering into a legally binding agreement.[229]

iv. Report Abuse Options

The Internet has become cluttered with "Report Abuse" options.[230] Various webpages invite users to report any unauthorized use of their identity or any unauthentic statements.[231] Wikipedia allows users to report inaccuracies in the content displayed.[232] Facebook permits people to report any content, including images as well as users, if they suspect that the content violates Facebook policies or their community standards.[233] Others like Amazon and eBay allow users to rate others and report fraud.[234] Similarly, PayPal conducts an investigation if any user reports that any buyer or seller has engaged in incomplete or fraudulent transactions.[235] If a buyer reports that a seller never shipped the products purchased, PayPal investigates the claim and takes reasonable measures, such as refunding the buyer's money.[236] Internet service providers that host pornographic content should utilize similar mechanisms of investigation and removal of certain unauthorized postings.

v. Display Identified Postings First

Another method that could be used by such providers could be that materials posted by identified posters are displayed first on the site, followed by anonymous postings.[237] Some websites currently have similar options available; such as when conducting a search for people, some social media sites display users with a profile image first. Users of pornographic materials are likely to view material that is displayed on the first few pages of a site, thereby leaving the posts that require flipping towards the last few pages with fewer views.

---

228. Kim, *supra* note 229, at 1015.

229. *Id.*

230. *Id.* at 1016.

231. *Id.*

232. *See generally* WIKIPEDIA (Aug. 24, 2014, 8:33 AM), http://en.wikipedia.org/wiki/Wikipedia:About;

233. *See generally* FACEBOOK (Aug. 24, 2014, 8:35 AM), https://www.facebook.com/about/privacy.

234. Kim, *supra* note 222, at 1016.

235. *See generally* PAYPAL (Aug. 24, 2014, 8:55 AM), https://www.paypal.com/us/webapps/helpcenter/helphub/home/.

236. *Id.*

237. Kim, *supra* note 222, at 1016.

vi. Time to Rethink

Another useful requirement enforced by service providers could include a "cooling off" period between the time a user uploads a post and the time it is posted for everyone to see.[238] Whenever a user posts potentially damaging material on a webpage, the website operators could be required by law to allow the user some time, from a few hours to a few days, to edit and remove the material before it is made visible to the public.[239] This cooling off period might cause a poster to rethink his actions and make the right decision.

vii. Warnings

Government legislation could require that owners of websites that host potentially damaging material shall post warnings on their home pages.[240] Just like warnings are mandated on drugs, movie DVDs, and at the start of certain adult-rated television shows, websites that supply space for potentially unauthorized pornographic material should be required to display similar warnings that inform the poster of the legal and non-legal dire consequences of posting non-consensual pornographic material. This warning will likely cause at least some culprits to make an informed decision and change their minds.[241]

viii. Maintenance of an Ethical Code of Conduct

If Internet service providers have been given immunity similar to the immunity available to media, the providers should be subject to certain ethical codes of conduct. Codes should be not be drafted by Internet service providers only; rather, they should be drafted by a joint effort of appropriate authorities, knowledgeable on the harms of Internet related offenses. Leaving the task of drafting the ethical code to ISPs would probably result in a biased code that is unlikely to be effective.

Ethical guidelines (similar to those enforced in Japan) that include provisions that forbid any defamatory posts on Internet bulletin boards are likely to provide relief to victims of defamation via the Internet in general, and victims of unauthorized sexual material in particular.

D. Required Notice and Take Down of Harmful Postings

Similar to the laws mandated by the European Union, United States government should draft legislation that imposes a duty on service providers to take down pornographic material once they are notified of its non-consen-

238. *Id.* at 1017.

239. *Id.*

240. *Id.*

241. *Id.* at 1118.

sual nature.[242] This legislation is possible by simply amending the CDA to include a duty to not only take down material that is claimed to be in violation of a copyright, but also material that is claimed to be distributed without the material's subjects's consent.

E. No Copyright Granted Without the Performer's Consent

The pornography industry has thrived arguably due to the economic incentive provided by copyright protection. Such protection should be available to the creator of the pornography only if he or she can provide the authorities with a written consent of the performers.[243] Additionally, copyright protection should be made available to not only the creators of the material, but each person that is shown in the material. This can be achieved by allowing copyright protection to the creator (if consent of the performers is provided), as well as the performers themselves in the same copyright grant. Each holder of the protection could sue another for unauthorized use of the material, but they cannot sue each other.

F. Non-Legal Remedies

There are assortments of non-legal remedies that can be made available to restrict revenge pornography instances and help the victims. Non-legal remedies have been employed by foreign countries such Japan and Singapore. Japan has a guideline for Internet use that ISPs and users of the web are expected to follow,[244] and in Singapore students are educated on Internet etiquette.[245] Although the focus of the paper is legal remedies, or the lack thereof, the following methods, if employed, could benefit society and protect us from the fear of what private aspect of our lives might appear on the global web for public view for generations.

i. Reputation Management Techniques[246]

The institution of reputation management services is not a new concept. Reputation harming websites are often accompanied by costly reputation management websites.[247] The techniques proposed here offer effective reputation management services that do not benefit the culprits and thereby remove some of the economic benefits derived by website owners who invite and encourage revenge pornography. These reputation management services

242. *See generally* Andy, *EU Court: ISPs can be forced to block pirate sites*, TORRENTFREAK.COM (Mar. 27, 2014), http://torrentfreak.com/eu-court-isps-can-be-forced-to-block-pirate-sites-140327/.

243. Bartow, *Copyright Law and Pornography*, *supra* note 81, at 799.

244. *See generally* Sterling, *supra* note 57, at 341.

245. *See generally id.*

246. Lipton, *supra* note 54, at 1149–50.

247. *See generally id.* at 1143.

would operate via public funding and offer pro bono services. Given the grim nature of the harm caused to victims of revenge pornography, such services could run on either government funding or public donations.

ii. Cyber Abuse Hotlines[248]

Cyber abuse hotlines are also not a recent phenomenon. The British Internet Watch Foundation provides a venue for the public to report illegal online conduct including obscenity, child abuse, child pornography, and racial hate materials.[249] The CyberTipline in the United States operates similarly but is only for reporting offenses pertaining to children.[250] Creating a hotline for reporting of potential non-consensual distribution of pornographic material would allow for communication of such offenses between victims, observers, and law enforcement officials. Hotlines can also provide information of websites to potential victims who suspect that an ex-lover has damaging material which he or she is likely to post online. They could check to see if damaging material that violates their privacy or reputation has been posted. This information will enable victims to timely seek reputation management services that can provide them with information, help them to take down the images, and take action against the offenders.

iii. Public Informational Messages

Public information campaigns have generally been successful in delivering messages that benefit a targeted audience or the public at large.[251] To date, such messages have dealt with issues of drug use, college access, gay-lesbian bullying, texting while driving, animal cruelty, and so on. Creating awareness of potential repercussions that follow any given course of conduct is a positive step towards managing the conduct. If people are made aware of the consequences of online bullying and revenge pornography, such as legal ramifications, psychological issues, irreparable damage to reputation and well-being, and subjecting the victim to potential sexual and physical assaults, to name a few, they will likely rethink their decisions to post destructive content.

G. Enactment of an International Law[252]

One of the hurdles to effectively catching the offenders that law enforcement officials face is the inability to charge the websites that induce defamation and harassment since the operators are often not within the jurisdiction of United States. Even though the Internet is not located in any one

248. *Id.* at 1150–51.

249. *Id.* at 1151.

250. *Id.*

251. *See generally id.* at 1140.

252. Sterling, *supra* note 57, at 349–50.

given space, and posts on the Internet have quick and global effects, offenders hide behind the jurisdictional limits of foreign countries as they simultaneously cause irreparable harm to those thousands of miles away. A universal international law that allows for the trial of a person or entity charged with the violation of distributing, or inducing a third party to distribute, non-consensual pornographic images would better serve the victims or potential victims. Under the proposed law, the actual poster as well as an ISP, who had notice of the non-consensual nature of the post or had reason to know that the service it provides will induce such posts, would be punished regardless of country and state lines.

Alternatively, a worldwide treaty could accomplish the same results. Under the treaty, because Internet posts cause injury to an individual, entity, or a group of individuals or entities, an ISP or individual poster would be subject to the defamation and harassment laws of multiple countries. Once again, like in case of an International Law, offenders would be greatly deterred by the prospect of facing liability-causing claims. For example, if a U.S. ISP, relying on his common law immunity, fails to remove images upon notice, or knows in all reasonable likelihood that its service would cause defamation or harassment, then a victim who faces damages from the ISPs in the United Kingdom could sue the ISP under victim-friendly British laws.

V. CONCLUSION

In the age of hackers and selfies, revenge pornography seems to be a predictable outcome, one that our legal system should have foreseen and adequately deterred. Revenge pornography has recently become a frequent topic for debate, as well as a cause for worry. Where people in the past dismissed the ever-present possibility of being victimized by statements such as "I would never trust anyone enough to allow cameras in the bedroom," the reality of being displayed on the Internet no longer shields the distrustful. With the advancements in hacking and social media websites, nearly anyone can succumb to the invasion of privacy.

"Leave it to Karma" may be an acceptable consolation when all else fails. Unfortunately, in this day and age Karma appears to be the only available recourse for victims who face great suffering at the hands of the legally invincible. Whereas various gossip blogs and celebrity magazines associate non-consensual "leaks" of pornographic videos as a tool for instant fame and the initial big break into stardom, the non-Paris Hiltons and non-Kim Kardashians of our times do not see this massive intrusion of privacy as any sort of blessing in disguise. As technology advances, it seems that fame, as well as a complete destruction of reputation and privacy are just a click away. Where vengeance once took months of planning and years to rear its ugly head, it now only takes an ex-lover or unknown enemy a few seconds to cause similar destruction with absolutely no fear of any dire consequences.

While the United States' legal system continually expresses its absolute disgust with the notion of prostitution and holds it to be a crime in most states, courts have accepted pornography as legitimate business, worthy of

legal protection. The act of engaging in sexual conduct for money is a crime, but when a camera records the acts, the "prostitute" becomes a subject of beneficial art, and the act goes from being a crime to a constitutionally guarded form of expression, one worthy of economic protection under copyright laws.

Although United States' strong commitment to First Amendment rights is what distinguishes it from other countries, it may be time to rethink the decision of holding First Amendment before the right to privacy, reputation, and expectation of common decency. The ability to watch and distribute pornography may be regarded by many as an American adult's fundamental right; however, is it really worth it when the right causes human trafficking, rape, difficulty in monitoring the ages of performers, emotional distress, and even suicides? Perhaps it is time to re-prioritize what is important.